REMARKS

I. INTRODUCTION

In response to the Office Action dated March 24, 2004, please consider the following remarks.

II. ALLOWABLE CLAIMS

In paragraph 14, the Final Office Action indicates that claims 4, 10, and 16 are allowable. The Applicants acknowledge and thank the Examiner for the identification of patentable subject matter, but traverse the rejection of the remaining claims for the reasons described below.

III. STATUS OF CLAIMS

Claims 1-8 and 10-19 are pending in the application.

Claims 1-3, 5-8, 11-15, and 17-19 were rejected under 35 U.S.C. §103(a) as being unpatentable over Benson, EP 0936530 (Benson) in view of Gabrielle, "USB Forum Produces Logo, Awareness Initiatives," 1997, Computer Retail Week, n 192, pg. 49 (Gabrielle).

IV. STATUS OF AMENDMENTS

No amendments to the claims have been made subsequent to the final Office Action.

V. ISSUES PRESENTED

Whether claims 1-3, 5-8, 11-15, and 17-19 are patentable under 35 U.S.C. § 103(a) over Benson in view of Gabrielle.

VI. GROUPING OF CLAIMS

The rejected claims do not stand or fall together. Each claim is independently patentable. Separate arguments for the patentability of each claim are provided below.

VII. ARGUMENTS

A. The Independent Claims Are Patentable Over The Prior Art

1. The Benson Reference

European patent applications EP 0 936 530 (hereinafter the Benson reference) discloses a virtual smart card. The virtual smart card emulates a real smart card by providing identical interface and services. The virtual smartcard has no physical manifestation and any smartcard-aware application can seamlessly interface with either a real smartcard or the virtual smartcard. A virtual smartcard server or duplication-protected physical media communicates with the virtual smartcard in order to activate or deactivate the virtual smartcard.

2. The Gabrielle Reference

"USB Forum Produces Logo, Awareness Initiative" by Gabrielle C. Mitchell, Computer Retail Week 1997, n. 192, pg. 49 (hereinafter, the Benson reference) is a news story about the use of USB-compliant devices.

3. The Subject Invention

The Applicants' invention is a compact, self-contained, personal key. The personal key comprises a USB-compliant interface releaseably coupleable to a host processing device operating under command of an operating system. Importantly, the token comprises (1) a smartcard processor having a smartcard processor-compliant interface for communicating according to a smartcard input and output protocol, and (2) an interface processor implementing a translation module for interpreting USB-compliant messages into smartcard processor-compliant messages and for interpreting smartcard processor-compliant messages into USB-compliant messages. These features provide specific advantages described in the Applicants' specification:

> First, smartcard processors 320 are relatively inexpensive and readily available. Second, a large number of application programs 110 have been developed for the use of smartcards, including the personal computer/smartcard (PC/SC) interface developed by the MICROSOFT CORPORATION. By providing a smartcard processor (which complies with the smartcard I/O protocols and supports smartcard command sets), this software can be used with a personal key 300 in a USB-compliant form factor. (Specification, page 10, lines 1-7)

With these features in mind, we now turn to the rejection of claims 1-19.

4. Independent Claim 1 is Patentable Over the Benson and Gabrielle References

Claim 1 recites:

> *a smartcard processor having a smartcard processor-compliant interface for communicating according to a smartcard input and output protocol;*
>
> *an interface processor, communicatively coupled to the USB-compliant interface and to smartcard processor-compliant interface the interface processor implementing a translation module for interpreting USB-compliant messages into smartcard processor-compliant messages and for interpreting smartcard processor-compliant messages into USB-compliant messages.*

As described below, even when combined, the Benson and Gabrielle references fail to disclose either a smartcard processor or an interface processor.

a) Benson and Gabrielle Fail to Disclose a Smartcard Processor

The First Office Action argued that the Benson reference discloses a token having a smart card processor as follows:

> As opposed to a physical smart card reader, a virtual smartcard reader 5 is virtual hardware acting as an emulator that passes information to and from a Virtual Smart Card 6. Additionally, the Virtual Smart Card Reader 5 communicates with a Virtual Smart Card Server 8 (VSC Server) via a network 7, e.g., an Intranet, Extranet, or the Internet. (col. 6, lines 38-45)
>
> The VSC Server 8 stores all protected information in its database (encrypted using the respective protection keys). When a Virtual Smart Card owner inserts a Virtual Smart Card 6, the VSC server 8 downloads the protected information; and when the owner removes a Virtual Smart Card 6, the Virtual Smart Card 6 uploads the updated protected information to the VSC Server 8. (col. 6, line 38 through col. 7, line 5)

The Applicants respectfully traversed, because the foregoing passages do not disclose a personal token having a smartcard processor, but rather, a Virtual Smart Card (VSC), which is essentially a smartcard emulator. Essentially, the Benson reference discloses a virtual smartcard, i.e. *software*, running on a general purpose processor, that emulates the behavior of a smartcard. The Applicants' invention, in contrast, uses a smartcard processor, not a smartcard emulator.

The Final Office Action responded that since the Applicants have not claimed a *physical* smartcard processor, this argument is moot.

The Applicants disagree.

The Final Office Action's interpretation of "smartcard processor" is improper. M.P.E.P § 2111 states that "During patent examination, the pending claims must be 'given the broadest reasonable interpretation *consistent with the specification*.'"

The specification is replete with references to the smartcard processor as a hardware device, and nowhere is it described as a software module or an emulator of any kind:

> First, to comply with USB interface protocol requirements, current USB-compliant personal keys utilize special purpose processors, instead of the low cost, limited capability processors currently available for smartcards. This increases the cost of the USB-compliant personal key, making widespread acceptance more difficult. Also, because each USB-compatible personal key may use a different processor (and different instruction sets), users may require different device drivers for different personal keys. This too represents another barrier to widespread acceptance of the personal key. (page 3, lines 8-15)

> From the foregoing, it is apparent that there is a need for a USB-compliant personal key that is usable with legacy personal identification devices, such as processors having smartcard processors and/or those complying with the ISO 7816. (page 3, lines 16-22)

FIG. 3 illustrates the smartcard processor 320, and is discussed in the text reproduced below:

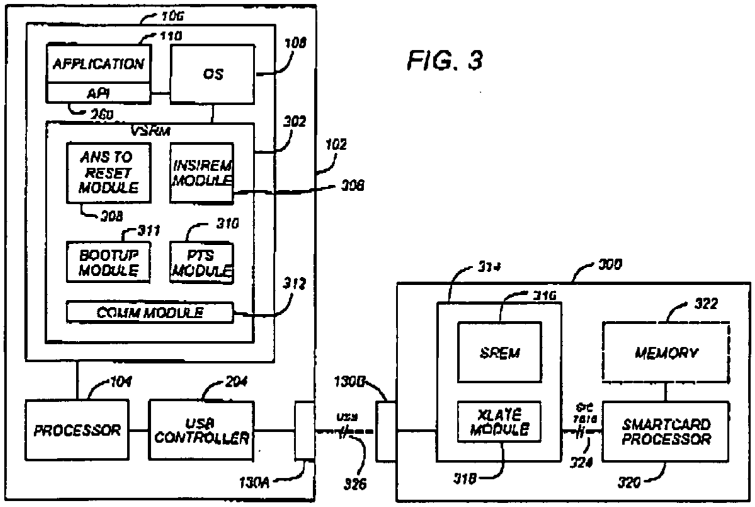


FIG. 3

> FIG. 3 is a block diagram of the personal key 300 and host computer 102 as applied to the present invention. Unlike the personal key 200 illustrated in FIG. 2, the personal key 300 illustrated in FIG. 3 comprises a smartcard processor 320. ***The smartcard processor 320 is a processor which complies with well-known smartcard I/O protocols and smartcard command sets and functions, such as those***

> ***described by the International Standards Organization (ISO) standard 7816 Part III (defining electronic properties and transmission characteristics), which is hereby incorporated by reference herein.***
>
> Physically, the smartcard compliant I/O interface 324 includes a serial I/O line, a reset (RST) line, a clock (CLK) line, a programming voltage (VPP), a power supply voltage (VCC) and a ground. This I/O interface 324 is further described in the publication "Introduction to Smartcards" by Dr. David B. Everett, which was published in 1999 by the Smart Card News Ltd., and is incorporated by reference herein.
>
> As was the case with the personal key 200 and host computer 102 illustrated in FIG. 1, the present invention allows the use of a personal key 300 communicating with the host computer 102 via a USB-compliant interface 130. ***However, the substitution of the smartcard processor 320 for the ordinary processor 212 depicted in FIG. 2 has several advantages. First, smartcard processors 320 are relatively inexpensive and readily available. Second, a large number of application programs 110 have been developed for the use of smartcards, including the personal computer/smartcard (PC/SC) interface developed by the MICROSOFT CORPORATION.*** By providing a smartcard processor (which complies with the smartcard I/O protocols and supports smartcard command sets), this software can be used with a personal key 300 in a USB-compliant form factor.(page 9, line 12 – page 10, line 7, emphasis added).
>
> ***The reset signal is used to start up the program contained in a memory 322 communicatively coupled to or resident within the smartcard processor 320.*** The ISO standard defines three reset modes, internal reset, active low reset, and synchronous high active reset. Most smartcard processors 320 operate using the active low reset mode. In this mode, the smartcard processor 320 transfers control to the entry address for the program when the reset signal returns to the high voltage level. The synchronous mode of operation is more commonly met with smartcards used for telephonic applications.
>
> ***The sequence of operations for activating the smartcard processor 320 is defined in order to minimize the possibility of damaging the smartcard processor 320. Of particular importance is avoiding corruption of the non-volatile memory 322 of the smartcard. Most smartcard processors 320 operate using an active low reset mode in which the smartcard processor 320 transfers control to the entry address for the program when the reset signal returns to the high voltage level. The sequence performed by the smartcard processor includes the steps of setting the RST line low, applying VCC to the proper supply voltage, setting the I/O in the receive mode, setting VPP in the idle mode, applying the clock, and taking the RST line high (active low reset).*** (page 12, lines 6-23, emphasis added)

FIG. 3 and the related discussion leads to the inescapable conclusion that the "smartcard processor" is indeed a hardware device: Further examples in the Applicants' specification abound.

The Final Office Action's interpretation of the "smartcard processor" as a non-physical device or a smartcard emulator is completely *inconsistent* with the specification, and is therefore impermissible under M.P.E.P. § 2111.

b) Benson and Gabrielle Fail to Disclose an Interface Processor

Claim 1 recites that the token comprises an interface processor and a translation module, which interprets USB-compliant messages into smartcard processor-compliant messages and interprets smartcard-compliant messages into USB-compliant messages. The First Office Action argued that Benson disclosed these features as follows:

> The VSC Server then permits the owner to use the Virtual Smart Card. When the Virtual Smart Card owner performs a remove operation, the Virtual Smart Card disables itself, securely sends a remove request to the VSC Server, and then shuts itself down. When the VSC Server receives a remove request, the VSC Server resets the Virtual Smart Card's state in the database to be idle.
>
> An alternative to the communication between the Virtual Smart Card and the Virtual Smart Card Server is presented in claim 10. The Virtual Smart Card Reader communicates with a dongle (or some other duplication-protected physical media). A duplication protected physical media has the property that it is exceedingly difficult for an unauthorized attacker to construct a copy of the media. The Virtual Smart Card is a copy protected program that executes only if permitted by the Dongle. If the end-user attaches the Dongle to the machine, then the Virtual Smart Card executes; otherwise, the Virtual Smart Card stops. (col. 4, lines 4-23).

and

> Insert 104: The end-user attaches the dongle 1101 and boots the Virtual Smart Card 6 program. The Virtual Smart Card 6 program does not operate unless the Virtual Smart Card 6 program can validate that the Dongle 1101 is present. The state of the Virtual Smart Card 6 is in-use 102 after the Virtual Smart Card 6 detects the Dongle 1101. This state is not explicitly recorded as in the case with the VSC Server 8. (col. 24, lines 8-16).

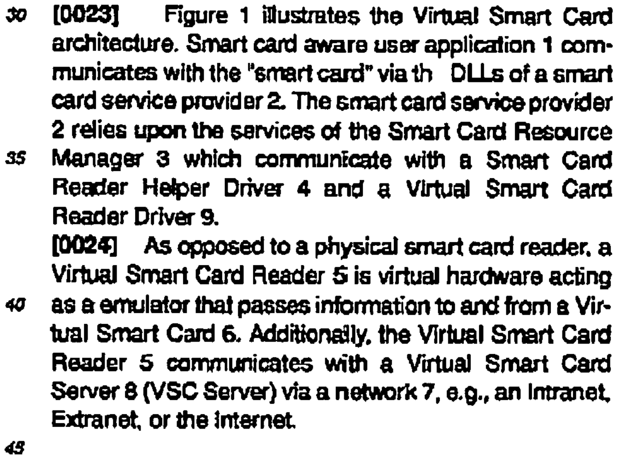
The Applicants disagreed, stating:

> "The foregoing describes the interaction between a the Virtual Smart Card and the Virtual Server (or, in col. 24, a Dongle). It does not describe a token with an interface processor, and does not describe an entity that is coupled between a smartcard processor and a USB-compliant interface, and does not describe any entity that interprets USB-compliant messages into smartcard-compliant messages or smartcard-compliant messages to USB-compliant messages. The Gabrielle reference is likewise deficient."

To which the Final Office Action replies:

> "Benson discloses a smartcard processor in a personal key (virtual smartcard) is enabled by use of an interface processor, because the interface processor includes a smartcard reader emulator, that functions to emulate those of a smartcard reader, thus projecting an image of a smartcard reader to the smartcard processor (see col. 6, lines 30-45).

The referenced portion of the Benson reference is reproduced below:



[0023] Figure 1 illustrates the Virtual Smart Card architecture. Smart card aware user application 1 communicates with the "smart card" via th DLLs of a smart card service provider 2. The smart card service provider 2 relies upon the services of the Smart Card Resource Manager 3 which communicate with a Smart Card Reader Helper Driver 4 and a Virtual Smart Card Reader Driver 9.

[0024] As opposed to a physical smart card reader, a Virtual Smart Card Reader 5 is virtual hardware acting as a emulator that passes information to and from a Virtual Smart Card 6. Additionally, the Virtual Smart Card Reader 5 communicates with a Virtual Smart Card Server 8 (VSC Server) via a network 7, e.g., an Intranet, Extranet, or the Internet.

Plainly, the foregoing does not disclose an *"interface processor, communicatively coupled to the USB-compliant interface and to smartcard processor-compliant interface the interface processor implementing a translation module for interpreting USB-compliant messages into smartcard processor-compliant messages and for interpreting smartcard processor-compliant messages into USB-compliant messages"*, as recited in claim 1.

Referring to the same portion of the Benson reference, the Final Office Action also states:

> "Benson also discloses that the virtual smartcard reader passes information to and from the virtual smartcard (see col. 6, lines 30-45). Therefore, the Examiner asserts that commands are sent and executed using a software emulation as done by Benson."

Of course, simply "passing information" does not teach the interface processor features recited in claim 1. The Applicants therefore respectfully traverse.

5. Independent Claim 8 is Patentable over the Benson and Gabrielle References

Claim 8 recites:

> *A host processing device, comprising:*
> *a processor;*
> *a memory, communicatively coupled to the processor, the memory storing processor operation commands implementing an operating system; and*

> *a virtual smartcard reader module stored in the memory and in communication with the operating system, for emulating at least one smartcard reader to the operating system, the virtual smartcard reader module comprising a communication module for packaging smartcard-compliant commands for transmission to a personal token communicatively coupled to the host processor via a USB-compliant interface and for unpacking smartcard-compliant responses received from the personal token.*

The First Office Action argued that these features were disclosed in the Benson reference as follows:

> As opposed to a physical smart card reader, a virtual smartcard reader 5 is virtual hardware acting as an emulator that passes information to and from a Virtual Smart Card 6. Additionally, the Virtual Smart Card Reader 5 communicates with a Virtual Smart Card Server 8 (VSC Server) via a network 7, e.g., an Intranet, Extranet, or the Internet. (col. 6, lines 38-45)
>
> The VSC Server 8 stores all protected information in its database (encrypted using the respective protection keys). When a Virtual Smart Card owner inserts a Virtual Smart Card 6, the VSC server 8 downloads the protected information; and when the owner removes a Virtual Smart Card 6, the Virtual Smart Card 6 uploads the updated protected information to the VSC Server 8. (col. 6, line 38 through col. 7, line 5)

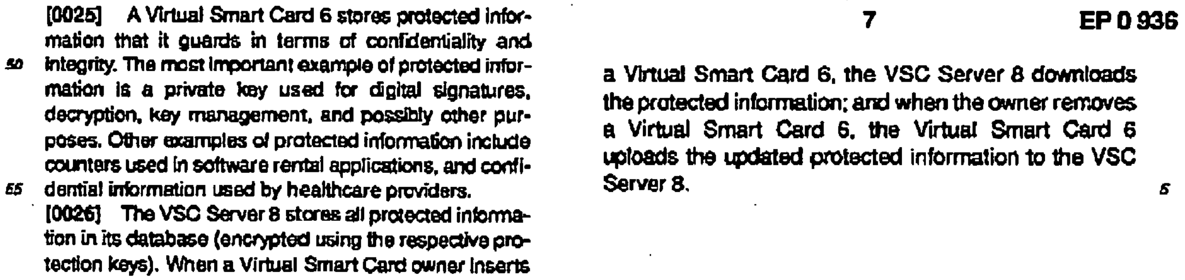
The Applicants traversed this rejection, because Benson does not disclose a virtual smartcard reader having a communication module packaging smartcard compliant commands to a personal token. As disclosed in Benson as follows, the "dongle" is used to authorize the execution of the Virtual Smart Card program:

> Figure 15 illustrates an alternative implementation of the Virtual Smart Card 6. This implementation does not require a VSC Server 8.
>
> Instead of communicating with the Virtual Smart Card Server 8 the Virtual Smart Card Reader 5 communicates with duplication-protected physical media, e.g., a Dongle 1101. A duplication protected physical media 1101 has the property that it is exceedingly difficult for an unauthorized attacker to construct a copy of the media 1101. The Virtual Smart Card 6 is a copy protected program that executes only if permitted by the Dongle 1101. If the end-user attaches the Dongle 1101 to the machine, then the Virtual Smart Card 6 executes; otherwise, the Virtual Smart Card 6 stops.(col. 23, lines 31-44)

Further, smartcard commands are not sent to either the Virtual Smart Card Server or the dongle. Instead, these entities act only as data repositories where protected data is stored and retrieved. There is no teaching to translate or package smartcard commands or responses.

Apparently acknowledging that there is no express teaching of a communication module in Benson, the Final Office Action argues that one is inherently disclosed:

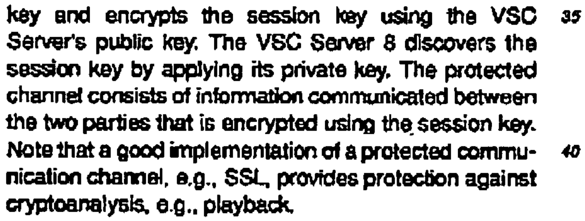
> "First, a communication module is inherent in Benson, because information is passed to virtual smart card reader from the virtual smart card (see col. 6, lines 38-45). The Applicant is urged to look further down column six. Benson discloses the virtual smart card stores protected information, such as digital signature. When the virtual smart card is inserted, the virtual smart card server downloads the protected information, thus there is a communication module in Benson (see col. 6, lines 48-58; col. 7, lines 1-5, col. 9, lines 38-41)"



7 EP 0 936

[0025] A Virtual Smart Card 6 stores protected information that it guards in terms of confidentiality and integrity. The most important example of protected information is a private key used for digital signatures, decryption, key management, and possibly other purposes. Other examples of protected information include counters used in software rental applications, and confidential information used by healthcare providers.

[0026] The VSC Server 8 stores all protected information in its database (encrypted using the respective protection keys). When a Virtual Smart Card owner inserts a Virtual Smart Card 6, the VSC Server 8 downloads the protected information; and when the owner removes a Virtual Smart Card 6, the Virtual Smart Card 6 uploads the updated protected information to the VSC Server 8.



key and encrypts the session key using the VSC Server's public key. The VSC Server 8 discovers the session key by applying its private key. The protected channel consists of information communicated between the two parties that is encrypted using the session key. Note that a good implementation of a protected communication channel, e.g., SSL, provides protection against cryptoanalysis, e.g., playback.

Of course, the issue isn't simply whether a "communication module" is disclosed in Benson or not … the issue is whether Benson discloses *"a communication module for packaging smartcard-compliant commands for transmission to a personal token communicatively coupled to the host processor via a USB-compliant interface and for unpacking smartcard-compliant responses received from the personal token"*, as recited in claim 1. A review of the cited portions of the Benson reference reveal that it does not. Accordingly, the rejection of claim 8 is traversed.

6. Independent Claim 14 is Patentable over the Benson and Gabrielle References

The First Office Action rejected claim 14 on the same basis as claims 1 and claim 3. The Applicants traversed this rejection for the reasons described above with respect to claim 1 and described below with respect to claim 3 (regarding whether Benson inherently discloses *a communication module for packaging messages for transmission to the personal token via the USB compliant interface according to a first protocol and for unpackaging messages received from the personal token via the USB-compliant interface according to the first protocol* and an *interface processor translation module unpackages messages from the host processing device according to the first protocol and packages messages destined for the host processing device according to the first protocol.*).

The Final Office Action offered no additional rationale for this rejection. Accordingly, the Applicants again traverse.

7. Independent Claim 19 is Patentable over the Benson and Gabrielle References

Claim 19 recites:

> *A virtual smartcard reader emulator system, comprising:*
> *a first smartcard reader emulator, implemented in a host computer for emulating smartcard reader operations to the host computer; and*
> *a second smartcard reader emulator, implemented in a personal key, for emulating smartcard reader operations to a smartcard-interface compliant personal key processor.*

The First Office Action argued that the foregoing features were disclosed in Benson as follows:

> The Virtual Smart Card Reader communicates with a Dongle (or some other duplication-protected physical media). A duplication-protected physical media has the property that it is exceedingly difficult for an unauthorized attacker to construct a copy of the media. The Virtual Smart Card is a copy protected program that executes only if permitted by the Dongle. If the end-user attaches the Dongle to the machine, then the Virtual Smart Card executes; otherwise, the Virtual Smart Card stops. (col. 4, lines 14-23)

and

> Insert 104: The end-user attaches the Dongle 1101 and boots the Virtual Smart Card 6 program. The Virtual Smart Card 6 program does not operate unless the Virtual Smart Card 6 program can validate that the Dongle 1101 is present. The state of the Virtual Smart Card 6 is in-use 102 after the Virtual Smart Card 6 detects the Dongle 1101. This state is not explicitly recorded as in the case with the VSC Server 8. (col. 24, lines 8-16)

Of course, nothing in the foregoing text suggests a smartcard reader emulator in a personal key for emulating smartcard reader operations to a smartcard-compliant personal key processor.

The Final Office Action provided no additional rationale and did not cite any further portions of either of the cited references. Accordingly, the Applicants traverse the rejection of claim 19.

B. The Dependent Claims Are Patentable Over The Prior Art

1. Dependent Claims 2-7, 10-13, and 15-18 are Patentable Over the Benson and Gabrielle References

Claims 2-7, 10-13, and 15-18 each recite the feature of the claims they depend upon and are patentable on the same basis. In addition, claims 2-7, 10-13, and 15-18 recite additional features rendering them even more remote from the prior art. Exemplary claims are discussed below:

With Respect to Claim 2: Claim 2 recites:

...wherein the interface processor emulates a smartcard reader to the smartcard processor.

According to the Office Action, Benson discloses that the interface processor emulates a smartcard reader to the smartcard processor as follows:

> The invention presents a bridge technology called Virtual Smart Card which emulates a real smart card by providing an identical interface and collection of services. ***However, the Virtual Smart Card has no physical manifestation.*** Any smart card-aware application can seamlessly inter-operate with either a real smart card or a Virtual Smart Card. (col. 3, lines 22-28, emphasis added)

and

> The Virtual Smart Card Reader communicates with a Dongle (or some other duplication-protected physical media). A duplication-protected physical media has the property that it is exceedingly difficult for an unauthorized attacker to construct a copy of the media. The Virtual Smart Card is a copy protected program that executes only if permitted by the Dongle. If the end-user attaches the Dongle to the machine, then the Virtual Smart Card executes; otherwise, the Virtual Smart Card stops. (col. 4, lines 14-23)

and

> As opposed to a physical smart card reader, a Virtual Smart Card Reader 5 is a virtual hardware acting as an emulator that passes information to and from a Virtual Smart Card 6. Additionally, the Virtual Smart Card Reader 5 communicates with a Virtual Smart Card Server 8 (VSC Server) via a network 7, e.g. an Intranet, Extranet, or the Internet. (col. 6, lines 38-44)

In response, the Applicants pointed out that VSC Reader disclosed above merely forwards emulated smart card messages unchanged to the VSC Server ... it does not "interpret USB-compliant messages into smartcard processor-compliant messages and for interpreting smartcard processor-compliant messages into USB-compliant messages", as claim 2 recites.

The Final Office Action merely reiterated this rejection. Accordingly, the Applicants respectfully traverse.

With Respect to Claim 3: Claim 3 recites that:

> *the host processing device comprises a virtual smartcard reader ... including a communication module for packaging messages for transmission to the personal token via the USB compliant interface according to a first protocol and for unpackaging messages received from the personal token via the USB-compliant interface according to the first protocol; and*
>
> *the interface processor translation module unpackages messages from the host processing device according to the first protocol and packages messages destined for the host processing device according to the first protocol.*

According to the First Office Action, the Benson reference discloses a virtual smartcard reader. The Office Action concedes that the Benson reference does not disclose a "communication module for packaging messages for transmission to the personal token via the compliant interface according to a first protocol" but asserts that this communication module is inherently disclosed.

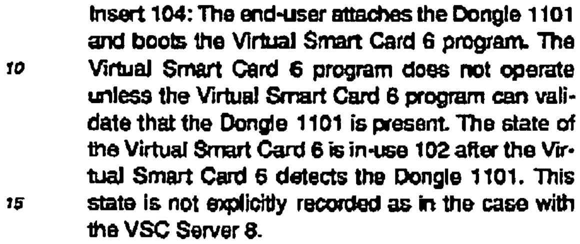
The Applicants respectfully disagreed, pointing out that Benson's Virtual Smart Card Reader interfaces directly with the Virtual Smart Card. Since both the reader and the smart card itself emulate smartcard processes and messages, there is no reason whatsoever for any sort of translation or packaging.

Inherency "may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient." *Continental Can Co. v. Monsanto Co.*, 948 F.2d 1264, 1269(Fed. Cir. 1991). Instead, to establish inherency, the extrinsic evidence "must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill." *Continental Can Co.*, 948 F.2d at 1268.

The Final Office Action responded:

> "The Examiner asserts that Benson inherently discloses this, because Benson discloses a virtual smart card reader that is a virtual hardware acting as a emulator that passes information to and from a virtual smart card (see col. 9, lines 38-41) and for unpacking messages received from the personal token via the compliant interface according to the first protocol, and the interface processor translation module unpackages messages from the host processing device according to the first protocol."

The cited portion of the Benson reference is reproduced below:



Insert 104: The end-user attaches the Dongle 1101 and boots the Virtual Smart Card 6 program. The Virtual Smart Card 6 program does not operate unless the Virtual Smart Card 6 program can validate that the Dongle 1101 is present. The state of the Virtual Smart Card 6 is in-use 102 after the Virtual Smart Card 6 detects the Dongle 1101. This state is not explicitly recorded as in the case with the VSC Server 8.

The Applicants fail to understand how the foregoing discloses the communication module and interface translation modules of claim 3. Accordingly, the rejection is traversed.

Regarding claims 6, 12, and 17: Claim 6 recites that the virtual smartcard reader (running in the host processing device) comprises a reporting module for receiving and reporting the insertion of the personal token in a USB-compliant port and the removal of the personal token as a removal of a smartcard from a smartcard reader. According to the First Office Action, Benson discloses these features as follows:

> Insert 104: The end-user attaches the Dongle 1101 and boots the Virtual Smart Card 6 program. The Virtual Smart Card 6 program does not operate unless the Virtual Smart Card 6 program can validate that the Dongle 1101 is present. The state of the Virtual Smart Card 6 is in-use 102 after the Virtual Smart Card 6 detects the Dongle 1101. This state is not explicitly recorded as in the case with the VSC Server 8. (col. 24, lines 8-16)
>
> At any time after successfully performing an insert operation, a Virtual Smart Card 6 may perform the remove operation (using the protected channel established during the insert operation). First, the Virtual Smart Card 6 disables itself by refusing all requests for services. Next, the Virtual Smart Card 6 sends a remove request to the VSC Server * which uploads the protected information (encrypted using the protection key). Upon receipt of a remove request, the VSC Server 8 resets its corresponding database entry to idle and returns a success acknowledgement. Next, the Virtual Smart Card 6 unlocks the local machine lock, zeros out the protected information, and shuts itself down. (col. 13, lines 41-53)
>
> Instead of communicating with the Virtual Smart Card Server 8, the Virtual Smart Card Reader 5 communicates with duplication-protected physical media, e.g., a Dongle 1101. (col. 23, lines 34-37)

Remove 105: The Dongle 1101 fails to authorize the Virtual Smart Card 6. For example, the end-user either removes the dongle 1101, or the Virtual Smart Card 6 shuts down. The state is idle 101 after the Dongle 1101 is removed. (col. 24, lines 18-22).

The Applicants traversed this rejection, as nothing in the foregoing passage appears to disclose a virtual smartcard reader having a reporting module reporting the insertion of the personal token in USB in a USB-compliant port and the removal of the personal token as a removal of a smartcard from a smartcard reader. At best, the foregoing independently describes a virtual smartcard performing remove operations and sending remove requests, and that the Virtual Smart Card shuts down if the user removes the dongle.

The Final Office Action merely reiterated this rejection. The Applicants therefore traverse.

VIII. CONCLUSION

In view of the above, it is submitted that this application is now in good order for allowance and such allowance is respectfully solicited. Should the Examiner believe minor matters still remain that can be resolved in a telephone interview, the Examiner is urged to call Applicants' undersigned attorney.

Respectfully submitted,

GATES & COOPER LLP
Attorneys for Applicant(s)

Howard Hughes Center
6701 Center Drive West, Suite 1050
Los Angeles, California 90045
(310) 641-8797

Date: May 24, 2004

By: ________________
Name: Victor G. Cooper
Reg. No.: 39,641

VGC/mrj